(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
28 juillet 2005 (28.07.2005)

PCT

(10) Numéro de publication internationale
WO 2005/069591 A1

(51) Classification internationale des brevets[7] :
H04M 1/725, G06F 1/00

(21) Numéro de la demande internationale :
PCT/EP2004/053523

(22) Date de dépôt international :
15 décembre 2004 (15.12.2004)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
03/15030 19 décembre 2003 (19.12.2003) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **THALES** [FR/FR]; 45, rue de Villiers, F-92200 NEUILLY SUR SEINE (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)* : **ERNY, Marie-Françoise** [FR/FR]; THALES, Intellectual Property, 31-33, avenue Aristide Briand, F-94117 CX ARCUEIL (FR). **BRETON, Sébastien** [FR/FR]; THALES, Intellectual Property, 31-33, avenue Aristide Briand, F-94117 CX ARCUEIL (FR).

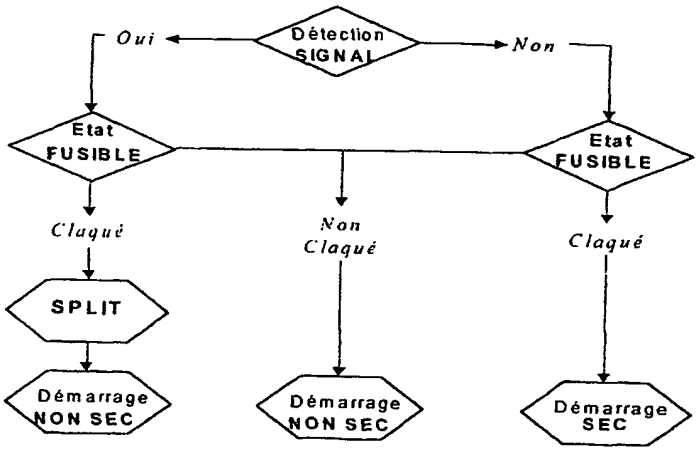
(74) Mandataires : **DUDOUIT, Isabelle** etc.; THALES, Intellectual Property, 31-33, avenue Aristide Briand, F-94117 ARCUEIL (FR).

(81) États désignés *(sauf indication contraire, pour tout titre de protection nationale disponible)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

[Suite sur la page suivante]

(54) Title: METHOD FOR DETECTING ILLEGAL MODIFICATIONS MADE TO MANUFACTURER SOFTWARE

(54) Titre : PROCEDE DE DETECTION DE MODIFICATIONS ILLICITES DES LOGICIELS CONSTRUCTEURS



(57) Abstract: The invention relates to a method enabling the detection and/or prevention of illegal modifications made to a manufacturer software in the field of a GSM system, comprising a hard core and a soft core, a local data interface, and having at least the following steps: A) when the signal received on the local data interface of the terminal is not valid, placing the GSM terminal in a non-operational state; B) the signal is a disconnecting signal on the local data interface, or when there is no signal, initiating a secured start-up procedure with the execution of the control functions: Autotest of the hard core: if the autotest is OK, test the integrity of the soft core; if this integrity is OK, activate the terminal for a normal operation; if the integrity is not OK, place the terminal in a non-operational state; if the autotest is not OK, place the GSM terminal in a non-operational state. C) the signal received is a valid start signal: if the fuse is not burnt out, make the GSM terminal operational; if the fuse is burnt out, make the terminal partially operational while deactivating at least one of the operational functions of the terminal: if the signal is a JTAG test signal, proceed with the test procedure; if the signal is a test signal, start in a non-secured mode and proceed with the test procedure.

[Suite sur la page suivante]

WO 2005/069591 A1

(84) **États désignés** *(sauf indication contraire, pour tout titre de protection régionale disponible)* : ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :
— *avec rapport de recherche internationale*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(57) Abrégé : Procédé permettant de détecter et/ou d'éviter des modifications illicites d'un logiciel constructeur au sein d'un système de type GSM, comprenant un noyau dur et un noyau mou, une interface locale de données, comportant au moins les étapes suivantes A - le signal reçu sur l'interface locale de données du terminal n'est pas valide, mettre le terminal GSM dans un état non opérationnel, B - le signal est un signal de déconnexion sur l'interface locale de données, ou il n'y a pas de signal, lancer une procédure de démarrage sécurisé, avec exécution des fonctions de contrôle Autotest du noyau dur, si l'autotest est OK, alors tester l'intégrité du noyau mou, si cette intégrité est OK, alors activer le terminal pour un fonctionnement normal, si l'intégrité est KO, alors mettre le terminal dans un état non opérationnel, si l'autotest est KO, alors mettre le terminal GSM dans un état non opérationnel. C - le signal reçu est un signal de démarrage valide, si le fusible est non claqué, rendre le terminal GSM opérationnel, si le fusible est claqué, rendre le terminal non totalement opérationnel, en désactivant au moins une des fonctions opérationnelles du terminal : si le signal est un signal de type test JTAG, poursuivre la procédure de test, si le signal est un signal de test, démarrer en mode non sécurisé et poursuivre la procédure de test.